



Sicherheits- & Datenschutz-Offenlegung, Abschlussbericht

WELT News Android (de.cellular.n24hybrid)

Ein hartcodierter Braze-CRM-Key exponiert die gesamte Nutzer-CRM-Infrastruktur von WELT, die Android Privacy Sandbox Topics API leitet aus politischer und gesundheitsbezogener Nachrichtenlektüre Werbe-Interessenprofile ab, und Tealium Tag Management sowie Google Mobile Ads initialisieren beide vor jeder Einwilligung, 74 Tage und neun Nachrichten lang unbeantwortet, 19 Tage nach Ablauf des Embargos, eine der drei ursprünglich adressierten Zustelladressen dauerhaft tot

**ÖFFENTLICHE OFFENLEGUNG, 17. OKTOBER 2026 — EMBARGO ERREICHT AM
28. SEPTEMBER 2026, VIER BEFUNDE UNBEANTWORTET**

Zielunternehmen	WeltN24 GmbH / Axel Springer SE, Berlin (XETRA: SPR)
Package	de.cellular.n24hybrid
Analysierte Plattform	Android, statische Analyse der Produktions-APK (35.837 Smali-Klassen)
Erstmeldung (R1)	2026-06-30 (REF WELT-2026-R1-001)
Offenlegungs-/Embargo-Datum	2026-09-28
Bericht veröffentlicht	2026-10-17
Gesamtschwere	CRITICAL
Befunde	4 (1 Critical, 3 High)
Korrespondenz	9 Nachrichten über 74 Tage an security@weltn24.de und datenschutz@axelspringer.com, 0 Antworten jeder Art, security@weltn24.de dreifach gebounced (moveoffice.com)
CC Behörden	Berliner Beauftragte für Datenschutz und Informationsfreiheit (BInBDI) · Europäischer Datenschutzbeauftragter (EDPS)

security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

1	Executive Summary	4
2	Gegenstand & Betreiber-Kontext	5
3	Korrespondenz-Zusammenfassung	5
4	Findings	5
4.1	C1: Firebase-API-Key, Produktions-DB-URL und Braze-CRM-API-Key hartcodiert	5
4.2	H1: ACCESS_ADSERVICES_TOPICS: Nachrichtenartikelkonsum wird zu Werbe-Interessenprofilen, mögliche Art. 9-Berührung	6
4.3	H2: Tealium Tag Management + Google Mobile Ads initialisieren beide vor Einwilligung (initOrder=100)	6
4.4	H3: Braze (765 Klassen) + Outbrain Native Ads: US-Transfer ohne erkennbaren Art. 44-49 Mechanismus	7
5	Impact-Analyse	7
6	Die vollständige Kette (The Complete Chain): Neun Nachrichten, 74 Tage, eine dauerhaft tote Adresse	8
7	Datenschutz — Artikel für Artikel (Data Protection)	8
8	Regulatorisches & rechtliches Umfeld (Regulatory)	9
9	Indicators of Compromise	9
10	Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis	10
11	Restrisiko & Empfehlungen (Residual Risk)	10

Executive Summary

WELT (ehemals N24) ist das digitale Nachrichten-Flaggschiff von Axel Springer SE (XETRA: SPR, ~€3,8 Mrd. Umsatz). Eine Root-Level-Analyse der Produktions-Android-App (de.cellular.n24hybrid, 35.837 Smali-Klassen) fand vier Befunde, einen CRITICAL und drei HIGH.

Ein Firebase-API-Key, die zugehörige Produktions-Datenbank-URL und ein Braze-CRM-API-Key sind hartcodiert in jeder installierten Kopie der App. Braze betreibt die vollständige Enterprise-CRM-Integration von WELT (765 Smali-Klassen: Push, In-App-Messaging, Behavioral Analytics, Nutzerprofile) — der exponierte Key legt diese gesamte Infrastruktur offen (C1). Die App deklariert zugleich die Android Privacy Sandbox Topics API, die aus dem Lesen von Nachrichtenartikeln hierarchische Werbe-Interessenprofile erstellt; auf einer Plattform, deren Nutzer politische Berichterstattung, Gesundheitsthemen und Migrationsdebatten konsumieren, kann dies Rückschlüsse auf politische Meinung oder Gesundheitszustand ermöglichen und damit DSGVO Art. 9 Sonderkategorien berühren (H1). Tealium Tag Management (lädt das vollständige Marketing-Tag-Stack) und Google Mobile Ads initialisieren beide mit `initOrder=100`, vor jeder Einwilligung (H2). Braze (765 Klassen) und Outbrain Native Advertising (9 Klassen), beide US-Dienstleister, verarbeiten Nutzerprofil- und Werbedaten ohne erkennbaren Art. 44-49 Transfermechanismus (H3).

RFI-IRFOS meldete diese Befunde am 30. Juni 2026 an security@weltn24.de und datenschutz@axelspringer.com, CC.presse@welt.de, die Berliner Datenschutzbehörde (BlnBDI) und den EDPS, mit Embargo-Datum 28. September 2026. Über die folgenden 74 Tage sendete RFI-IRFOS acht weitere Nachrichten; drei davon bounceten dreifach an security@weltn24.de (moveoffice.com-Infrastruktur), worauf diese Adresse aus den Folge-nachrichten entfernt wurde. Über neun Nachrichten insgesamt wurde keine einzige Antwort jeder Art empfangen, von keiner der beiden verbleibenden Adressen, auf keiner Ebene von Axel Springer SE.

ID	Severity	Title
C1	CRITICAL	Firestore-API-Key, Produktions-DB-URL und Braze-CRM-API-Key hartcodiert
H1	HIGH	ACCESS_AD SERVICES_TOPICS: Nachrichtenartikelkonsum wird zu Werbe-Interessenprofilen, mögliche Art. 9-Berührung
H2	HIGH	Tealium Tag Management + Google Mobile Ads initialisieren beide vor Einwilligung (<code>initOrder=100</code>)
H3	HIGH	Braze (765 Klassen) + Outbrain Native Ads: US-Transfer ohne erkennbaren Art. 44-49 Mechanismus

Gegenstand & Betreiber-Kontext

WELT ist Axel Springers digitales Nachrichten-Flaggschiff, in direkter redaktioneller Konkurrenz zu BILD und anderen Axel Springer-Marken. Die Topics-API-Befunde dieses Berichts sind in diesem Kontext besonders relevant: WELT-Leser konsumieren tagesaktuelle politische Berichterstattung, deren Kategorisierung durch eine Werbeprofiling-API eine andere Risikoklasse darstellt als dieselbe Technik auf einer unpolitischen Plattform.

Korrespondenz-Zusammenfassung

RFI-IRFOS sendete die Erstmeldung am 30. Juni 2026 an security@weltn24.de und datenschutz@axelspringer.com, CC presse@welt.de, die Berliner Datenschutzbehörde (BlnBDI) und den EDPS, mit Embargo-Datum 28. September 2026 unter REF WELT-2026-R1-001. Folgenachrichten gingen am 17. Juli, 27. Juli und 4. August 2026 jeweils an beide Adressen; jede dieser drei Sendungen wurde für security@weltn24.de von postmaster@moveoffice.com als unzustellbar zurückgewiesen. Ab der Nachricht vom 9. August 2026 wurde security@weltn24.de aus der Empfängerliste entfernt und nur noch datenschutz@axelspringer.com direkt adressiert; weitere Folgenachrichten gingen am 12. August, 15. August, 31. August und 12. September 2026. Über neun Nachrichten und 74 Tage hinweg wurde keine einzige Antwort jeder Art empfangen, auch keine automatische Bestätigung.

Findings

C1: Firebase-API-Key, Produktions-DB-URL und Braze-CRM-API-Key hartcodiert

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:H/SI:N/SA:N, 8.3

```
google_api_key:      [REDACTED IN PUBLIC REPORT -- disclosed privately to WELT/Axel
  Springer in R1]
firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to WELT/Axel
  Springer in R1]
braze_api_key:       [REDACTED IN PUBLIC REPORT -- disclosed privately to WELT/Axel
  Springer in R1]
```

Braze-Integrationstiefe: 765 Smali-Klassen (volle Enterprise-CRM-Plattform)

Impact: RFI-IRFOS blast-radius escalation: von HIGH/8.3 auf CRITICAL angehoben, weil der exponierte Braze-Key nicht nur einen einzelnen Dienst, sondern die vollständige CRM/Marketing-Automation-Infrastruktur (765 Smali-Klassen) für WELTs gesamte Leserschaft offenlegt. google_api_key, firebase_database_url und braze_api_key sind in res/values/strings.xml hartcodiert und damit in jeder installierten APK-Kopie enthalten. Braze ist mit 765 Smali-Klassen als vollständige Enterprise-CRM-Plattform integriert (Push-Notifications, In-App-Messaging, Behavioral Analytics, Nutzerprofile). Der exponierte Braze-Key stellt damit nicht nur ein einzelnes Datenbank-Quota-Risiko dar, sondern exponiert Segmente, Kampagnen und Nutzerprofil-Daten der gesamten WELT-CRM-Infrastruktur.

H1: ACCESS_ADSERVICES_TOPICS: Nachrichtenartikelkonsum wird zu Werbe-Interessenprofilen, mögliche Art. 9-Berührung**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.8**

```
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_TOPICS"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_AD_ID"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_ATTRIBUTION"/>
```

Inferierte Beispiel-Topics aus Artikelkategorien: "News & Politics", "Health", "Society"

Impact: Die App deklariert ACCESS_ADSERVICES_TOPICS, ACCESS_ADSERVICES_AD_ID und ACCESS_ADSERVICES_ATTRIBUTION. Die Android Privacy Sandbox Topics API erzeugt aus App-Nutzungsverhalten hierarchische Werbe-Interessenprofile (z. B. 'Nachrichten & Politik', 'Gesundheit', 'Gesellschaft'). Auf WELT als politischer Nachrichtenplattform bedeutet dies: Leser von Gesundheitspolitik-Berichten generieren das Topic 'Health', Leser politischer Kommentare das Topic 'News & Politics', Leser von Migrationsdebatten eine politische Interessen-Inferenz. Soweit aus dem Leseverhalten Rückschlüsse auf politische Meinung, Gesundheitszustand oder Religionszugehörigkeit möglich sind, berührt dies DSGVO Art. 9(1) Sonderkategorien, ohne dass eine Art. 6(1)-Rechtsgrundlage oder eine Art. 35 DSFA für diese spezifische Konfiguration erkennbar ist.

H2: Tealium Tag Management + Google Mobile Ads initialisieren beide vor Einwilligung (initOrder=100)**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:H/SI:N/SA:N, 7.1**

```
<provider android:name="com.tealium.core.internal.TealiumInitProvider"
    android:initOrder="100"/>
<provider android:name="com.google.android.gms.ads.MobileAdsInitProvider"
    android:initOrder="100"/>
```

Einwilligungssignal vor Initialisierung erfasst: nein

Impact: com.tealium.core.internal.TealiumInitProvider und com.google.android.gms.ads.MobileAdsInitProvider sind beide mit android:initOrder=100 deklariert und initialisieren damit vor dem Einwilligungsbildschirm. Tealium TMS lädt beim Start das vollständige Marketing-Tag-Stack (Werbenetzwerke, Analytics, Tracking); Google Mobile Ads ist das Werbeschaltungs-SDK. Beide beginnen mit der Datenverarbeitung, bevor der Nutzer irgendeine Einwilligung erteilt hat.

H3: Braze (765 Klassen) + Outbrain Native Ads: US-Transfer ohne erkennbaren Art. 44-49 Mechanismus

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 7.4

Braze CRM: 765 Smali-Klassen (New York, USA)

Outbrain: 9 Smali-Klassen (New York, USA)

Dokumentierter Art. 44-49 Transfermechanismus: keiner identifiziert

Impact: Braze (New York, 765 Smali-Klassen) verarbeitet Nutzerprofil-, Verhaltens- und Push-Engagement-Daten; Outbrain (New York, 9 Smali-Klassen) ist eine Native-Advertising-Plattform. Beide sind US-Dienstleister; ein Art. 44-49 DSGVO Transfermechanismus für diese Datenflüsse ist nicht erkennbar.

Impact-Analyse

C1 ist der schwerwiegendste Befund, weil der exponierte Braze-Key nicht ein isoliertes Secret ist, sondern den Zugriffsschlüssel zur vollständigen CRM-Infrastruktur (765 Klassen) eines großen Nachrichtenmediums darstellt. H1 verschärft sich durch den redaktionellen Kontext von WELT selbst: politische Tagesberichterstattung, die über die Topics API in Werbe-Interessenprofile überführt wird, bewegt sich strukturell näher an DSGVO Art. 9 als dieselbe Technik auf einer unpolitischen App. H2 und H3 sind konventionellere, aber wiederkehrende Gaps (Pre-Consent-Initialisierung, US-Transfer ohne Mechanismus), die zusammen mit C1 und H1 ein Muster fehlender Datenschutz-Governance auf einer der größten deutschen Nachrichten-Apps zeichnen.

Durchgängig zeigt sich dasselbe Korrespondenzmuster wie in anderen Fällen dieser Offenlegungs-Serie: neun Nachrichten über 74 Tage produzierten keine einzige Antwort jeder Art, von keiner Seite Axel Springers.

Die vollständige Kette (The Complete Chain): Neun Nachrichten, 74 Tage, eine dauerhaft tote Adresse

Schritt 1 — Meldung gesendet: RFI-IRFOS sendet den vollständigen Befundbericht am 30. Juni 2026 an security@weltn24.de und datenschutz@axelspringer.com, CC presse@welt.de, BlnBDI und EDPS, mit Embargo-Datum 28. September 2026.

Schritt 2 bis 4 — Drei Folgenachrichten, dreifacher Bounce: Am 17. Juli, 27. Juli und 4. August 2026 sendet RFI-IRFOS Folgenachrichten an beide Adressen; alle drei werden für security@weltn24.de von postmaster@moveoffice.com als unzustellbar zurückgewiesen. datenschutz@axelspringer.com bouncet zu keinem Zeitpunkt.

Schritt 5 — Adresse entfernt: Ab der Nachricht vom 9. August 2026 wird security@weltn24.de aus der Empfängerliste entfernt.

Schritt 6 bis 9 — Vier weitere Folgenachrichten: Am 12. August, 15. August, 31. August und 12. September 2026 gehen weitere Nachrichten ausschließlich an datenschutz@axelspringer.com. Keine davon wird beantwortet.

Schritt 10 — Embargo erreicht und überschritten: Das am 30. Juni 2026 einmalig genannte Embargo-Datum verstreicht am 28. September 2026, alle vier Befunde unbeantwortet.

Schritt 11 — Veröffentlichung: Dieser Bericht erscheint 19 Tage nach dem Embargo-Datum. Über 109 Tage und neun Nachrichten an eine durchgehend funktionierende Adresse enthält die Korrespondenz null Antworten jeder Art.

Datenschutz — Artikel für Artikel (Data Protection)

Art. 32(1)(b), Art. 25 DSGVO — Sicherheit der Verarbeitung, Datenschutz durch Technikgestaltung: C1s hartcodierte Keys exponieren die vollständige CRM-Infrastruktur ohne erkennbare Schutzmaßnahme.

Art. 5(1)(b), Art. 13, Art. 6(1), ggf. Art. 9 DSGVO — Zweckbindung, Transparenz, Rechtsgrundlage, Sonderkategorien: H1s Topics-API-Konfiguration überführt Nachrichtenkonsum in Werbepprofile ohne erkennbare Rechtsgrundlage für diese Zweckänderung.

Art. 7 DSGVO — Bedingungen für die Einwilligung: H2s Tealium- und Mobile-Ads-Initialisierung erfolgt vor jeder Einwilligung.

Art. 28, Art. 44-49 DSGVO — Auftragsverarbeitung, Drittlandtransfer: H3s Braze- und Outbrain-Integration hat keinen dokumentierten Transfermechanismus für den US-Datenfluss.

Regulatorisches & rechtliches Umfeld (Regulatory)

Axel Springer SE (XETRA: SPR) ist eines der größten Medienhäuser Deutschlands; WELT ist dessen digitales Nachrichten-Flaggschiff. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) sowie der Europäische Datenschutzbeauftragte (EDPS) wurden über die ursprüngliche Meldung und jede Folgenachricht informiert (DSGVO Art. 83(2)(b)).

Bußgeldrahmen nach DSGVO: Art. 83(5) ist auf die potenzielle Art. 9-Berührung in H1 anwendbar, bis zu 20.000.000 € oder 4 % des weltweiten Jahresumsatzes. Art. 83(4) ist auf C1, H2 und H3 anwendbar, bis zu 10.000.000 € oder 2 % des weltweiten Jahresumsatzes. Dass ein Unternehmen dieser Größenordnung auf neun schriftliche Meldungen über 74 Tage nicht reagiert, auch nicht automatisiert, ist ein Faktum, das eine Aufsichtsbehörde neben den vier technischen Befunden mit abwägen dürfte.

Indicators of Compromise

Die folgenden Identifikatoren, SDK-Pakete und Manifest-Deklarationen wurden ausschließlich durch statische Analyse der Produktions-APK extrahiert. Es wurden keine WELT-, Axel Springer-, Braze- oder Outbrain-Server, -Konten oder -Infrastruktur geprüft.

```
C1 -- google_api_key, firebase_database_url, braze_api_key: [REDACTED IN PUBLIC REPORT  
    -- disclosed privately to WELT/Axel Springer in R1]  
  
H1 -- android.permission.ACCESS_AD_SERVICES_TOPICS  
    android.permission.ACCESS_AD_SERVICES_AD_ID  
    android.permission.ACCESS_AD_SERVICES_ATTRIBUTION  
  
H2 -- com.tealium.core.internal.TelemInitProvider (initOrder=100)  
    com.google.android.gms.ads.MobileAdsInitProvider (initOrder=100)  
  
H3 -- Braze CRM: 765 Smali-Klassen  
    Outbrain: 9 Smali-Klassen
```

Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis

2026-06-30 Erstmeldung an security@weltn24.de und datenschutz@axelspringer.com, CC presse@welt.de, BlnBDI, EDPS. Embargo: 2026-09-28. REF WELT-2026-R1-001.

2026-07-17, 2026-07-27, 2026-08-04 Drei Folgenachrichten; security@weltn24.de bouncet jedes Mal über postmaster@moveoffice.com. datenschutz@axelspringer.com bouncet nie.

2026-08-09 security@weltn24.de aus der Empfängerliste entfernt, ab hier nur noch datenschutz@axelspringer.com direkt adressiert.

2026-08-12, 2026-08-15, 2026-08-31, 2026-09-12 Vier weitere Folgenachrichten. Keine Antwort jeder Art an irgendeinem Punkt.

2026-09-28 Embargo-Datum erreicht, wie am 2026-06-30 einmalig genannt und nie revidiert. Korrespondenz-Stand: neun RFI-IRFOS-Nachrichten, null Antworten jeder Art.

2026-10-17 Dieser Bericht veröffentlicht, 19 Tage nach dem Embargo-Datum.

Restrisiko & Empfehlungen (Residual Risk)

C1 — Sofort: hartcodierte Firebase- und Braze-Keys im Produktions-Build rotieren und aus dem Quellcode in eine sichere Secrets-Verwaltung verschieben.

H1 — Sofort: entweder ACCESS_ADSERVICES_TOPICS entfernen oder eine eigenständige, dokumentierte Art. 6(1)-Rechtsgrundlage und Art. 35 DSFA für die Überführung von Nachrichtenartikeln in Werbe-Interessenprofile schaffen, mit besonderem Augenmerk auf mögliche Art. 9-Berührung.

H2 — Kurzfristig: Tealium- und Mobile-Ads-Initialisierung hinter die Einwilligungentscheidung legen, statt mit initOrder=100 vor dem Consent-Screen zu starten.

H3 — Kurzfristig: einen Art. 44-49-Transfermechanismus für Braze- und Outbrain-Datenflüsse dokumentieren und in der Datenschutzerklärung ausweisen.

Alle Befunde — security@weltn24.de als Kontaktpfad für Sicherheitsmeldungen überprüfen oder abschalten: eine dreifach gebouncete Sicherheits-Kontaktadresse bei einem Unternehmen dieser Größe ist ein eigenständiger Prozessfehler, unabhängig von den vier technischen Befunden dieses Berichts.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria Alle Befunde beruhen auf statischer Analyse der

veröffentlichten Anwendung mittels öffentlich verfügbarer Werkzeuge. Es wurden keine WELT-, Axel Springer-, Braze- oder Outbrain-Server, -Konten oder -Infrastruktur geprüft. Technische Nachweise sind unter Chain of Custody archiviert und werden Aufsichtsbehörden auf Anfrage zur Verfügung gestellt. Forschung durchgeführt gemäß ISO/IEC 29147, der Freiheit der Wissenschaft (Art. 17 StGG) und DSGVO Art. 89. REF WELT-2026-R1-001.